Business Technology Alignment
First Architecture Support Group (ASG) Review Document

Version 1.0
February 1, 2002

Task Order #85

Deliverable # 85.1.3

Overview

The Business Technology Alignment (BTA) scope within the SFA Modernization effort focuses on supporting closer alignment of technology-related issues with business priorities, and the standardization and management of the SFA technical infrastructure.

SFA's BTA framework utilizes a pragmatic, "just in time" approach to the development of technical architecture standards. The approach is to develop and recommend technical standards on an as-needed basis for the specific project need while taking an enterprise perspective. The technical standard development effort is triggered by a business need identified, usually in the context of a development project, and the standards are scoped, identified and agreed driven by the specific project need, but based on the most appropriate benefits and tradeoffs from a SFA-wide perspective. Within SFA's process for definition of technical standards, the ASG review is a critical milestone. This milestone provides the basis for agreeing recommendations to be made to the Architecture Working Group (AWG) – which represents the business units – for acceptance of the standards. These recommendations are captured in a white paper, developed as part of the analysis and recommendations phase, and agreed during the review.

SFA's technical standards development process is summarized below:

Technical Standards Development Process Summary

Phases	**1. Issue Identification and Scoping**	**2. Analysis and Recommendation**	**3. Acceptance**	**4. Implementation and Documentation**
Activities	• Identify need for standard • Scope the issue	• Sponsor analysis • Assign responsibility for analysis • Conduct analysis • Prepare "whitepaper" • Perform due diligence: **ASG Review**	• Select option (if appropriate): AWG Review • Request additional analysis, or accept recommendation(s)	• Document and communicate new standards • Implement recommended solution(s)

This paper contains supporting documents that facilitated the ASG Review of the recommendations, held on January 23, 2002, proposing technical standards for encryption of sensitive data.

Architecture Support Group (ASG) Review Summary

This set of documents summarize the outcome of the Architecture Support Group (ASG) review examining the recommendations for setting encryption standards for certain specified data transmission modes. These recommendations are being forwarded to the Architecture Working Group (AWG) for ratification and business unit agreement.

This deliverable consists of the following two documents:

- Minutes of the ASG Review held on January 23, 2002

- Recommendations by the ASG For the Protection of Transmitted Data Whitepaper

Business Technology Alignment (BTA)
ASG Meeting Minutes: January 23, 2002

Location:	830 1st Street, NW, WDC (room 221C), 11:00 –12:00
Present:	Andy Boots, SFA Bill Bush, SFA David Elliott, SFA Jim Greene, SFA Robert Laurence, DTI Ganesh Reddy, SFA Gary Adams, CSC Karen Anderson, Mod Partner Michael Bruce, Mod Partner Bill Hughes, Mod Partner Bob Malloy, Mod Partner Bill Malyszka, Mod Partner Paul Peck, Mod Partner Michael Sauser, CSC Jamal Shah, Mod Partner RayThomas, CSC
Objective and Agenda:	Objective: Agree recommendations for Encryption Technical Standards for discussion and agreement by the Architecture Working Group (AWG). Agenda: □ Introduction & Context Setting □ Recommendation of Encryption Technical Standards o Issue o Recommendations o Options Evaluated o Pros and Cons of each o Discussion (gaps, other options, etc) □ Other Issues □ Recommendation(s) to the AWG
Issues/Risks:	Need to clarify and recommend policy addressing security of data transmission from existing systems.
Next Meeting:	**TBD**

Meeting Discussion Items:

- Introduction & Context Setting
    - Purpose of the meeting was to review the recommendations that have been developed, identify any gaps or issues, and agree recommendations to be made to the AWG in setting data security/ encryption standards.
- Recommendation of Encryption Technical Standards

  The discussion centered around the following topics:

    - Document terms

      The term “ application to application” should be modified to show that the intent of the phrase was to apply to data transferred from within an SFA firewall to outside of that firewall.

    - AWG
        - The white paper recommends certain standards that the AWG should review, understand the implications of from a business unit perspective, and either agree with, or request additional information on, if appropriate.
        - The AWG will need to provide guidance on how to address particular issues, such as addressing the data security needs of legacy systems.
    - Scope
        - The encryption standards do not need to address transactions occurring within the same data center.
        - The white paper should include a discussion of topologies, their differences, and the risks.
        - Standards for certain transactions have not been addressed in the white paper, and will need to be addressed on an as-needed basis. These include:
            - Legal or agency requirements (e.g. FIPS, financial transactions with Department of Treasury, lock box treatment, etc.).
            - Data compression (COMPRESS within B-TRADE).
            - Hardware based encryption.
        - Current effort does not need to inventory all of the existing systems for compliance level.
    - Policy
        - The recommendations imply the need to address and create a policy for existing non-compliant systems (e.g. “grand-fathering” or time intervals for compliance). This needs to be included as a discussion topic with the AWG.
        - Premise is that the recommendations should be a help aid for development and not something to enforce limitations on new projects.

- Business channels need to assess the security risk to their data.
    - Issue: many business unit representatives believe that they are using T1 lines, when in fact they are using frame relay, which has a different risk level than they perceive.
- The document raises the issue of how to continue doing business with agencies that have no security standard (eg VA)

- Recommendation to the AWG
    - Standards as described in white paper.
    - Request guidance on:
        - Addressing legacy systems; potential options:
            - Initiate effort to inventory legacy systems and recommend how to address, based on economics and business priorities and risk.
            - Legacy systems exempt from compliance with new standards.
            - All systems must comply with security standards by specified date, e.g. October 2003, or have obtained a waiver.
        - Addressing need for compliance with Federal standards.

SFA Modernization Program

United States Department of Education

Student Financial Assistance

Recommendations by the ASG
For the
Protection of Transmitted Data
Whitepaper

Version 2.0

January 30, 2002

Document Revision History

Version No.	Date	Author	Revisions Made
0.1	January 15, 2002	Michael Bruce	Discussion draft for Enterprise Architecture Core working group review
0.2	January 18, 2002		Working Draft recommendation for ASG review
1.0	January 23, 2002	Mike Bruce, Karen Anderson, Bill Malyszka, Jamal Shah	Draft recommendation for AWG review
2.0	January 30, 2002	Mike Bruce, Karen Anderson, Bill Malyszka, Jamal Shah, David Elliott, Andy Boots	Incorporated feedback from the ASG meeting held on January 24.
2.0	January 31, 2002	Karen Anderson	Renamed title page from ‘Date Protection Solutions for the ASG Recommendations’

Table of Contents

Introduction

SFA's BTA framework utilizes a pragmatic, "just-in-time" approach to the development of technical architecture standards. The approach is to develop and recommend technical standards on an as-needed basis for the specific project need while taking an enterprise perspective. Thus, when a need for a SFA technical standard is identified by a project, an effort is initiated to identify options, conduct the necessary analysis and make recommendations driven by the needs of that particular project, but based on the most appropriate benefits and tradeoffs from a SFA-wide perspective. This focuses the effort and the limited resources where they are most needed and will make the greatest impact, while continuing to populate SFA's technical standards guide.

This document describes the issue triggering the need for identification of application data encryption standards. It then summarizes the recommendations, the potential options and the analysis leading to the recommendations.

This document addresses recommendations only for encryption standards for particular transmission modes, and does not address all the data security needs for all transmission modes at SFA. It is expected that technical standards recommendations will be developed for security of data utilizing the remaining transmission modes as, and when, they are needed.

Context

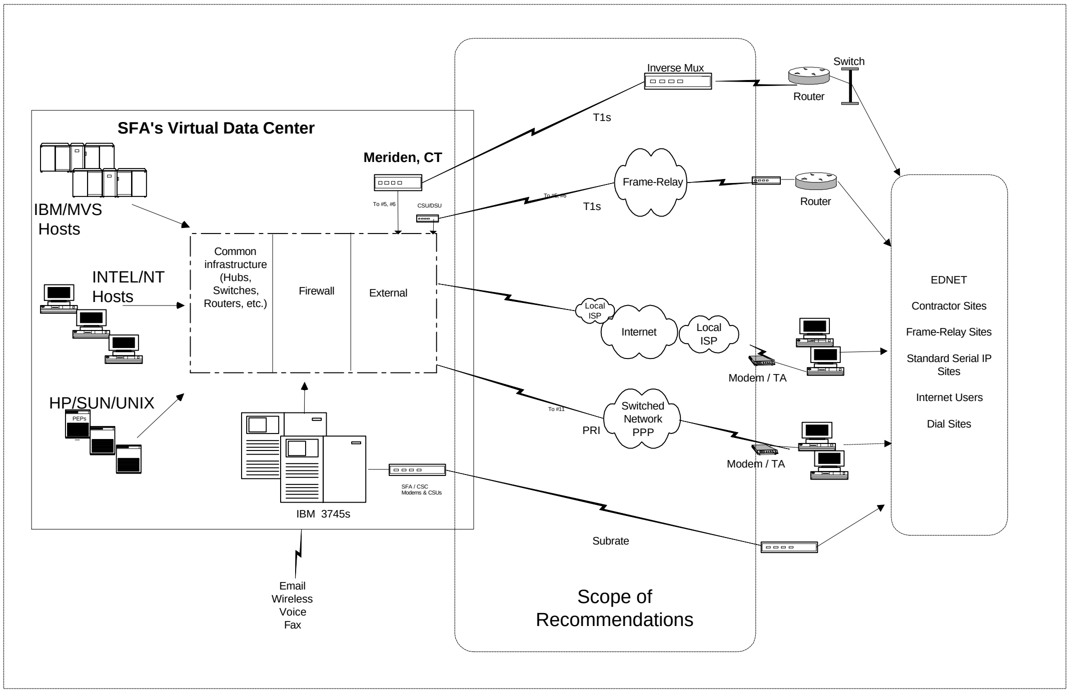
The need for secure application data has triggered this investigation of options for establishing a pertinent standard. The necessity for the standard arose from the eServicing project. The Architecture Working Group (AWG) of the SFA has requested the Architecture Support Group (ASG) to provide a recommendation regarding technical enterprise standards for protecting Privacy Act application data intended for transmission. This request follows the procedures of the Business Technology Alignment (BTA) framework developed by SFA.

Major Applications and General Support Systems hosted at the SFA data centers often transmit confidential information to other external systems and users of the Public Switched Telephone Network (PSTN) or the Internet. When unauthorized access of this information can harm the Department, it must be protected during transmission. Securing the confidentiality and integrity of this information is an important element of SFA's business operations.

This information may be stored within SFA systems, transmitted between SFA systems, or transmitted from SFA systems to customers and business partners.

System managers, system security officers, and development partners need to utilize common services, practices, and processes to protect information. As SFA re-engineers applications, develops new applications, and introduces externally managed applications, development teams require a standard set of approved data protection options which can meet application/system requirements and which are part of SFA's business/technology architecture. These options must protect data 'Confidentiality', 'Integrity', 'Availability', and 'Accountability' for information that is 'Processing', 'At Rest', and 'In-Transit'.

The illustration below provides a pictorial view of the SFA technical environment.



Scope

SFA system managers require standard procedures to encrypt and protect sensitive application data that is transmitted to meet their overall business needs. This document provides proposed recommendations for:

- Data transmissions between the SFA and external systems through the PSTN.
- Application-to-application transmission.
- Application-to-end user via the Internet.

This document does not address the data transmitted over the following communication protocols:

- E-mail
- Wireless
- Voice
- Fax

These represent future topics to be addressed by the Architecture Working Group.

Assessing the Need for Securing Data

The unauthorized release of such confidential information poses potential business, financial, operational, political, public image, and other risks to SFA. Systems managers and application development leads must assess applications and data (both input and output) to determine the level of data protection required in the transmission of information. For existing major applications and general support systems, the Office of the Chief Information Officer (OCIO) has completed an inventory of systems which categorizes them by:

- *Type* (Major Application or General Support System)
- *Mission Criticality* (Critical, Important, Supportive)
- *Data Sensitivity** (High, Medium, Low)

Based on the assessed level of risk, system managers must determine the proper and prudent mechanisms for protecting information within the applications and systems they are responsible. Managers responsible for a new system can compare it to similar systems, which have been assessed, for guidance in identifying the new system's level of risk.

*(*See Appendix A: Federal, Department of Education, & SFA Policy for high, medium and low definitions)*

Descriptions of Possible Solutions

The following are solutions for the encryption of confidential application data transmitted and received by SFA systems:

1) <u>Virtual Private Network (VPN)</u>
Data can be transmitted from point to point using VPN software; uses a certificate to encrypt and decrypt data.

2) <u>Secure Socket Layer (SSL)</u>
Using a server certificate (i.e., private key) the application server encrypts data prior to external transmission, and a browser certificate (i.e., public key) decrypts data upon receiving an encrypted transmission.

3) <u>Firewall Encryption</u>
Data is encrypted as it transverses the network firewall, forwarded to a destination address, and decrypted at the firewall of the receiving entity.

4) <u>Hardware Router Encryption</u>
Data is encrypted as it is processed by the router (i.e., hardware based VPN), forwarded to a destination address, and decrypted as it is received.

5) <u>Application Encryption</u>
The system can encrypt data prepared for transmission or store data as encrypted records.**Technical Recommendations**

Below are recommended solutions for encrypting data that is transmitted by SFA mission critical applications in various situations. Any one of these efforts can be designed to use either Point to Point, Cloud (Frame Relay/ATM), Intranet, Internet/Extranet. The technical lead can determine the data transfer method for existing systems and can provide a technical architecture for new systems. There are different products available from a range of vendors that provide the functionality of the recommended solutions.

1) Data transmission to and from external data centers via the PSTN.
SFA applications that need to transmit information from one application hosted within the SFA data center that handles, stores and processes Privacy Act and confidential data, to another application hosted outside the SFA data center, should utilize router level encryption to protect the confidentiality and integrity of in-transit information.

   Rationale: Hardware router level encryption provides a SFA data center wide solution that will be available to any application hosted by the SFA data centers. For data centers receiving SFA data, this provides the most effective option from an implementation and operations perspective. Based on SFA data centers and Modernization Partner analysis this was the solution recommended by the COD initiative.

2) Application-to-application via the Internet.
SFA applications transmitting information over open networks (via HTTP or FTP) to and from an application external to the originating data center should use SSL (Secure Socket Layer) data encryption to protect confidential information. The industry standard within the United States is 128-bit encryption and should be used. Outside the United States 40-bit encryption[1] should be used except in countries to which the United States allows higher bit levels of data encryption.

   Rationale: SSL encryption is the industry standard for application to end-user secure data transfer via the Internet. SSL implementation is well understood and supported by all major vendors of Internet and web application server products (IBM Websphere products).

3) Application-to-end user via the Internet.
SFA applications transmitting information over open networks (via HTTP or FTP) to and from a user external to the originating data center should use SSL (Secure Socket Layer) data encryption to protect confidential information. The industry standard within the United States is 128-bit encryption and should be used. Outside the United States 40-bit encryption[1] should be used except in countries to which the United States allows higher bit levels of data encryption.

   Rationale: SSL encryption is the industry standard for application to end-user secures data transfer via the Internet. SSL implementation is well understood and supported by all major vendors of Internet and web application server products (IBM Websphere products).

Although these recommendations are suitable in the majority of instances, an application may have a specialized need for alternative data encryption protocols. For example, technical architects may want to consider using PKI (Public Key Infrastructure) to encrypt data. Such alternatives will be reviewed by the ASG for recommendation to the AWG as an SFA enterprise standard on a case-by-case basis.

Basis For Recommendation

Emerging project needs require capabilities that do not have technical standards defined to support them. There are two projects (COD and eServicing) that have the requirement to transmit confidential application data. These teams have conducted the necessary research to select application data encryption procedures that follow industry best practices and standards, and satisfy federal and SFA data security policies. The analyses conducted in the following projects were used as a basis for the recommendations in this document: COD for SFA data center encryption recommendations; eServicing for data protection over the Internet.

The analyses are summarized in Appendix B: COD and eServicing Encryption.

Implications of Recommendations**Existing Systems**

It is recommended that the business owner reevaluate their applications to determine the sensitivity of their data and decide if data protection is warranted. The business wonders will need to be aware to the potential organizational risks associated with each decision If the business owner find their high risk data is not protected, the business owner will be required to apply for a security waiver.**New Systems**

The matrix below can be used to map the data protection and transfer method to the level of data confidentiality. The below table categorizes each potential solution by the level of security it may provide and the circumstances for which it may be suited. (See Appendix A: Federal, Department of Education, & SFA Policy for high, medium and low definitions)

Transfer Method	***Data Sensitivity***		
	High	***Medium***	***Low***
Point-to-Point	*Hardware Router Encryption*	*Hardware Router Encryption*	*None*
Cloud (Frame Relay/ATM)	*SSL Session Encryption*	*SSL Session Encryption*	*None*
Intranet	*SSL Session Encryption*	*SSL Session Encryption*	*None**
Internet/Extranet	*SSL Session Encryption*	*SSL Session Encryption*	*None**

*(*SSL may still be advisable to assure customers they are dealing with legitimate SFA site).*

The following chart illustrates the options for application data encryption. Based on the merits of each option and the application's business and technology requirements, appropriate options from this list are recommended above as the SFA standard for application implementation.

Option	Description	Implementation Alternatives	Costs	Pros	Cons
Secure Socket Layer	Information is encrypted by certificate technology by the application server	Secure Socket Layer (SSL)	Server Certificate one-time and recurring fees Application integration development cost	• Can be used by any application server • Efficient for online user to application transactions • An industry and SFA 'de facto' standard	• Must be implemented on an application by application basis • Not suitable for transmission of large bulk file
Virtual Private Network (VPN)	Information can be transmitted point-to-point using VPN software. Uses digital certificates to encrypt/decrypt information.	Requires VPN software from a COTS provider	VPN software and hardware, example: WorldCom Dedicated Access: Dial-up $1,500/mo plus $19.95/mo per user and a onetime install fee. Dedicated connection $595/mo for 56 Kbps; $1,895/mo for 1.544 Mbps; and $35.5K/mo for 45 Mbps. Customer Managed: $3K setup, Cisco router ranging from US$4.6K to $29.5K, and $1.8K/mo per site for T1 up to $90K/mo OC-3.	• Allows information requestor to be authenticated. • Data cannot be viewed without the appropriate decryption key. Can be used for remote secure access. • Can be used for bulk data transfer.	• VPN has not yet been implemented at SFA. • Requires an investment in hardware, software, and training. • Performance degradation due to need to utilize VPN service to encrypt and decrypt all information transmitted over the network. • Installation and deployment can be difficult.

Option	Description	Implementation Alternatives	Costs	Pros	Cons
Application Encryption	Information is encrypted by applications. Applications created encrypted files for transmission or store encrypted records.	Requires encryption software on application server. RSA - Bsafe in use by eServicing.	RSA BSAFE product suite – $295 per copy for SDK, Runtime license XX Application development – cost per application	• Allows information resident in any data store (e.g., file, database, memory, etc.) to be encrypted.	• Encryption software may not be compatible with all applications. • Development projects and existing applications must implement this solution on an application-by-application basis. • Requires changes to application code and processing. • Systems receiving transmission requires compatible decryption algorithm.
Firewall Encryption	Information is encrypted at the firewall as it is transmitted externally.	Nokia / CheckPoint encryption software	Nokia / CheckPoint $55,509 annual SFA data center costs (Estimate for COD and 3 remote locations)	• Scalable solution allows for growth. • Straightforward installation. • Provides a shared enterprise resource.	• All locations require compatible firewall encryption software. • Additional hardware devices required at remote locations for data to traverse and SFA data centers to operate. • Costs grow as the number of remote locations increases.

Option	Description	Implementation Alternatives	Costs	Pros	Cons
Router Encryption	Information is encrypted by router hardware/software as it is transmitted externally.	Cisco 7206 VXR Routers with encryption hardware	Cisco Router $73,636 annual SFA data center costs (Estimate for COD and 3 remote locations)	• Scalable solution allows for growth. • Good performance. • Best economies of scale as use increases. • Provides a shared enterprise resource.	• All locations require compatible router hardware. • Need to upgrade and replace SFA data center production hardware.

Appendixes

Appendix A: Federal, Department of Education, & SFA Policy

The following policies provide guidance regarding the protection of confidential information. The procedures used to protect information must adhere to these policies:

1) Privacy Act (1974, as amended)

   a) Agencies must "establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."

2) OMB Circular A-130, Management of Federal Information Resources (November 28, 2000):

   a) The individual's right to privacy must be protected in Federal Government information activities involving personal information.

   b) Agencies will ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information;

3) 3) SFA Policy ():

   a) Confidential information should be protected in a manner appropriate to the sensitivity of the information. This applies to information in transit and in storage. It is the responsibility of the business unit to determine the appropriate method of protection.

   b) SFA has adopted SSL as the 'de facto' acceptable method to protect information transmitted over open networks (via HTTP or FTP).

The following information has been extracted from the Department of Education General Support Systems and Major Applications Inventory Guide document, December 31, 2001.

To appropriately protect information, its relationship to and impact on the mission of the Department must be understood. Therefore, it is necessary to know the requirements of the data to be protected from specific risks to apply appropriate security controls.

The National Institute for Standards and Technology (NIST), in its Self Assessment Guide (SP 800-26), uses three basic protection requirements in order to determine the information sensitivity -- confidentiality, integrity (which, for the purposes of the Guide, includes non-repudiation and authenticity), and availability.

- Confidentiality – Protection from unauthorized disclosure
- Integrity – Protection from unauthorized, unanticipated, or unintentional modification
- Non-repudiation – Verification of the origin or receipt of a message
- Authenticity – Verification that the content of a message has not changed in transit
- Availability – Available on a timely basis to meet mission requirements or to avoid substantial losses.

Each area must be rated on the scale of High, Medium, or Low, using the following guidance from NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, and NIST SP 800-26, *Self Assessment Guide for Information Technology Systems,* for making the determination.

- **High:**
  - A critical concern for the automated information resource
  - Extremely grave injury accrues to U.S. interests if the information is compromised; could cause loss of life, imprisonment, major financial loss, or require legal action for correction.
- **Medium:**
  - An important concern, but not necessarily paramount in the organization's priorities
  - Serious injury to U.S. interests if the information is compromised; could cause significant financial loss or require legal action for correction.
- **Low:**
  - Some minimal level of security is required, but not to the same degree as the previous two categories.
  - Injury accrues to U.S. interests if the information is compromised; would cause only minor financial loss or require only administrative action for correction.

In making the determination of the level of protection required for each of the three areas of confidentiality, integrity, and availability, additional factors should be considered, including:

- The amount of human and capital investment dedicated to the GSS or application
- Refer to the 17 control areas reviewed in NIST SP 800-26 to determine if any supplemental security controls have been applied to the GSS or application.

Confidentiality

To determine the appropriate level for confidentiality, consider the needs of the information to be protected from unauthorized disclosure. Consideration should also be given to data requiring protection under the Privacy Act and financial and proprietary data. As an example, identify theft could result from the unauthorized disclosure of personal information used by the Department. If the data contains Privacy Act, financial, or proprietary information, the GSS or application should receive a classification of no less than Medium. If the data contains social security numbers, the GSS or application should receive a classification of no less than High.

The following examples from NIST SP 800-18 can be used as guidance in making this determination.

Example Confidentiality Considerations

High

The application contains proprietary business information and other financial information, which if disclosed to unauthorized sources, could cause unfair advantage for vendors, contractors, or individuals and could result in financial loss or adverse legal action to user organizations.

Medium

Security requirements for assuring confidentiality are of moderate importance. Having access to only small portions of the information has little practical purpose.

Low

The mission of this GSS or application is to provide general information to the public. None of the information requires protection against disclosure.

Integrity

To determine the appropriate level for integrity, consider the needs of the information to be protected from unauthorized, unanticipated, or unintentional modification. This includes, but is not limited to, consideration of authenticity, non-repudiation, and accountability (requirements can be traced to the originating entity). As an example, the nature of the loan information processed by the Department may cause it to be targeted for unauthorized modification.

The following examples from NIST SP 800-18 can be used as guidance in making this determination.

Example Integrity Considerations

High

The application is a financial transaction system. Unauthorized or unintentional modification of this information could result in fraud, under or over payments of obligations, fines, or penalties resulting from late or inadequate payments, and loss of public confidence.

Medium

Assurance of the integrity of the information is required to the extent that destruction of the information would require significant expenditures of time and effort to replace. Although corrupted information would present an inconvenience to the staff, most information, and all vital information, is backed up by either paper documentation or on disk.

Low

The GSS or application mainly contains messages and reports. If these messages and reports were modified by unauthorized, unanticipated, or unintentional means, employees would detect the modifications; however, these modifications would not be a major concern for the organization.

Availability

To determine the appropriate level for availability, consider the needs of the information to be available on a timely basis to meet mission requirements or to avoid substantial losses. Availability also includes ensuring that resources are used only for intended purposes.

The availability requirement should be based on the period of operation during which the GSS or application is most critical for the business function to be conducted. For instance, if a GSS or application operates only one month a year, consider the availability requirement for that month.

The following examples from NIST SP 800-18 can be used as guidance in making this determination.

Example Availability Considerations

High

The application contains personnel and payroll information concerning employees of the various user groups. Unavailability of the application could result in inability to meet payroll obligations and could cause work stoppage and failure of user organizations to meet critical mission requirements. The application requires 24-hour access.

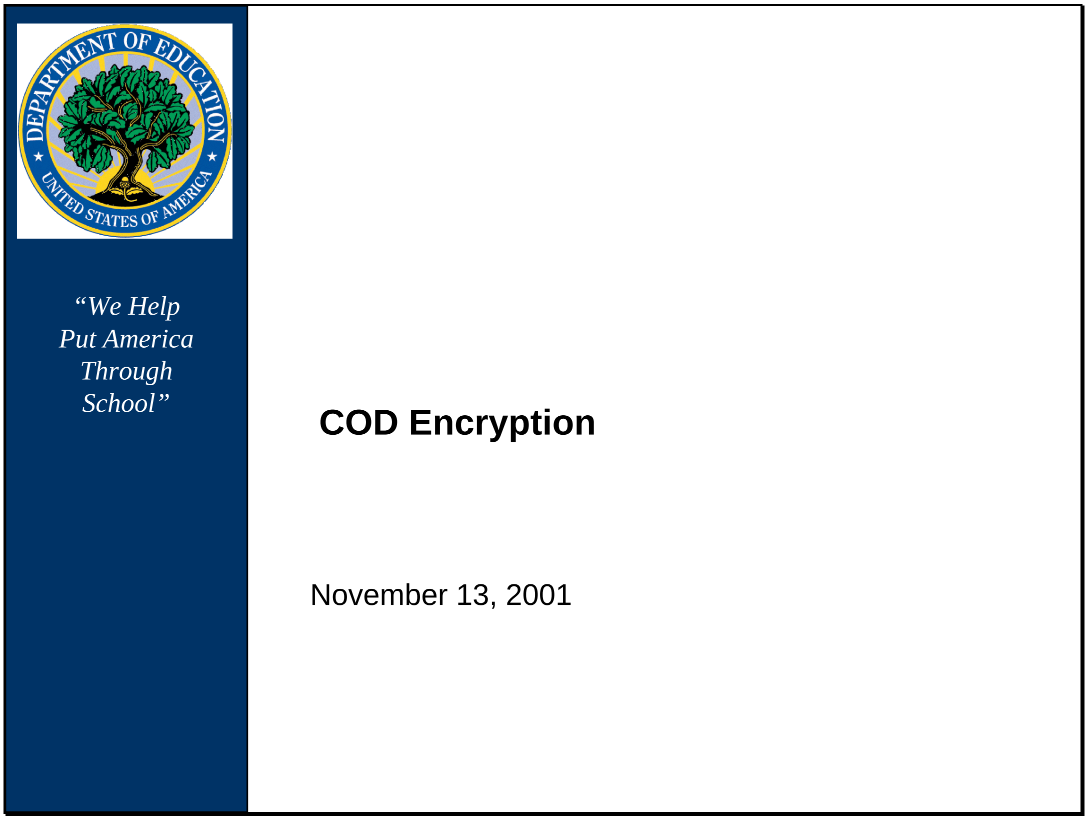
Medium

Information availability is of moderate concern to the mission. Availability would be required within the four to five-day range. Information backups maintained at off-site storage would be sufficient to carry on with limited office tasks.

Low

The GSS or application has a duplicate from which the information can be accessed and processed, causing no interruption in the continuity of business functions.

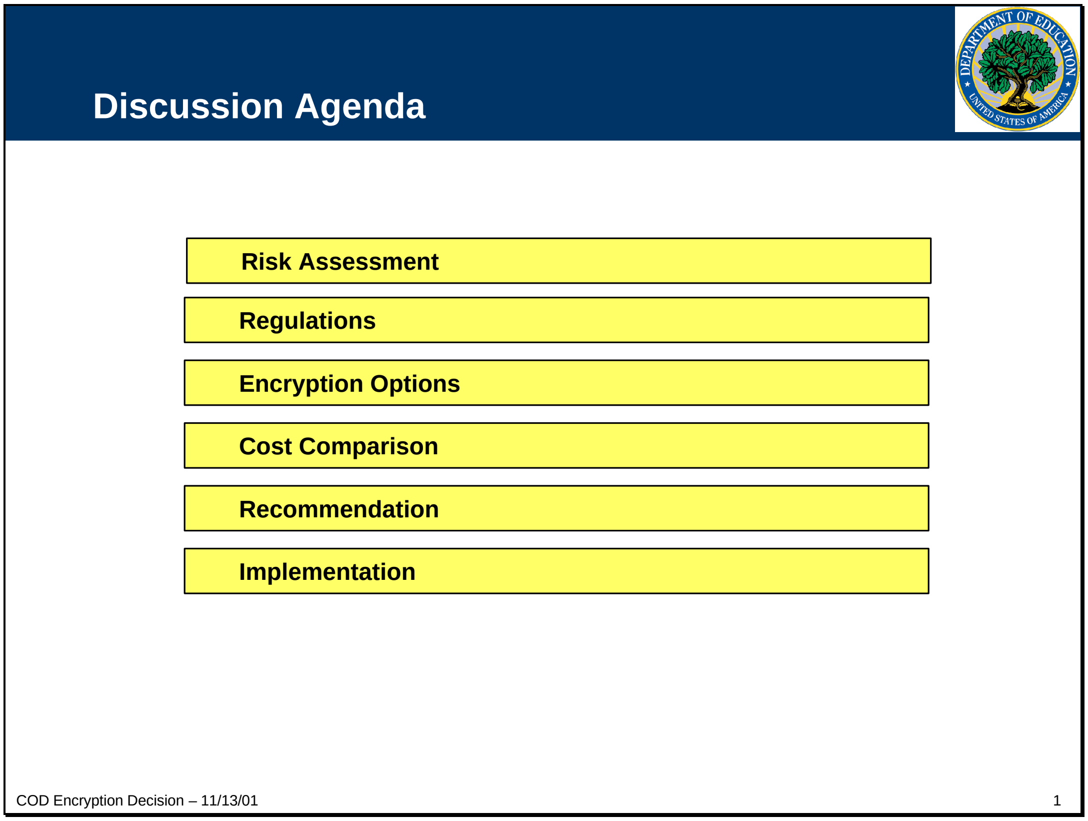
Appendix B: COD and eServicing Encryption Assessment



“We Help
Put America
Through
School”

COD Encryption

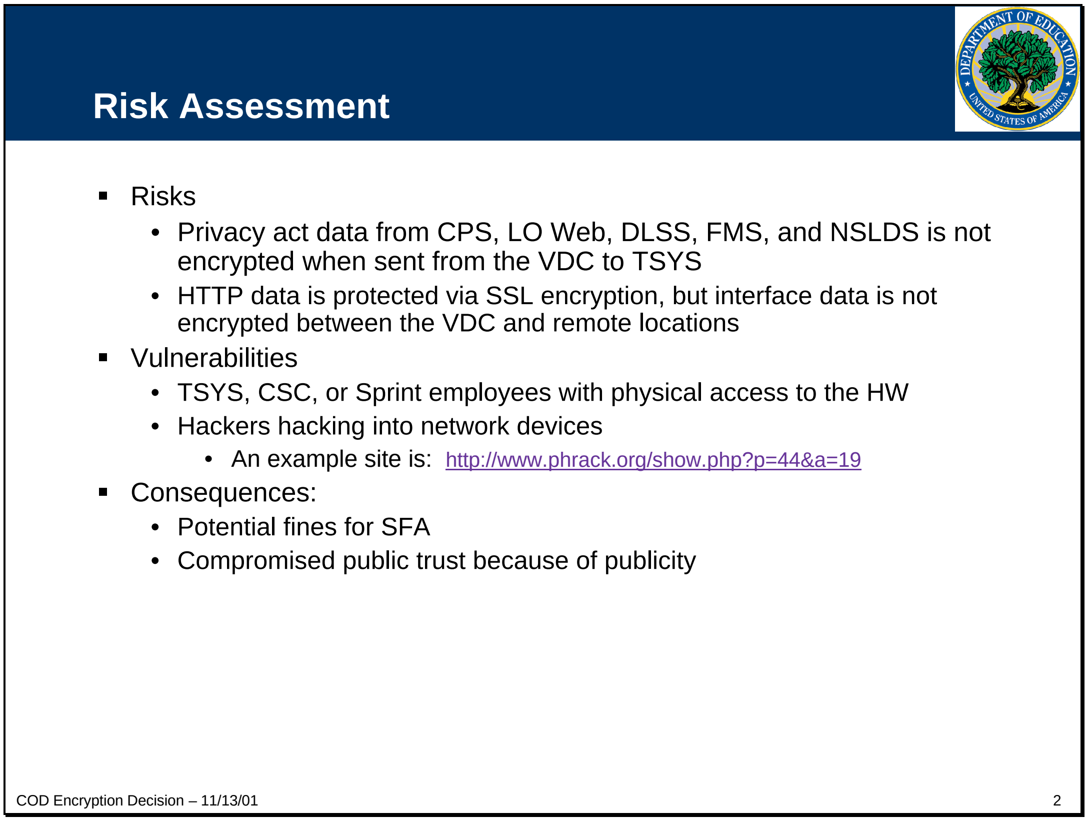
November 13, 2001



Discussion Agenda

- Risk Assessment
- Regulations
- Encryption Options
- Cost Comparison
- Recommendation
- Implementation

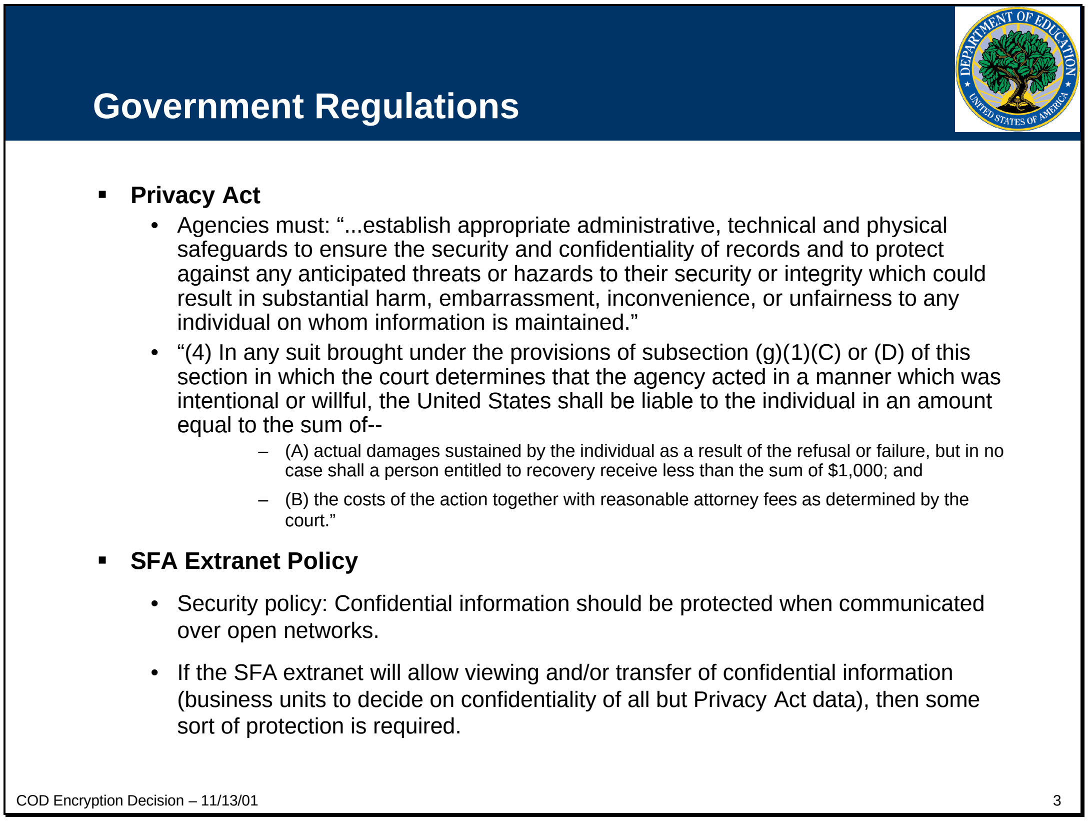
COD Encryption Decision – 11/13/01 1



Risk Assessment

- Risks
  - Privacy act data from CPS, LO Web, DLSS, FMS, and NSLDS is not encrypted when sent from the VDC to TSYS
  - HTTP data is protected via SSL encryption, but interface data is not encrypted between the VDC and remote locations
- Vulnerabilities
  - TSYS, CSC, or Sprint employees with physical access to the HW
  - Hackers hacking into network devices
    - An example site is: http://www.phrack.org/show.php?p=44&a=19
- Consequences:
  - Potential fines for SFA
  - Compromised public trust because of publicity

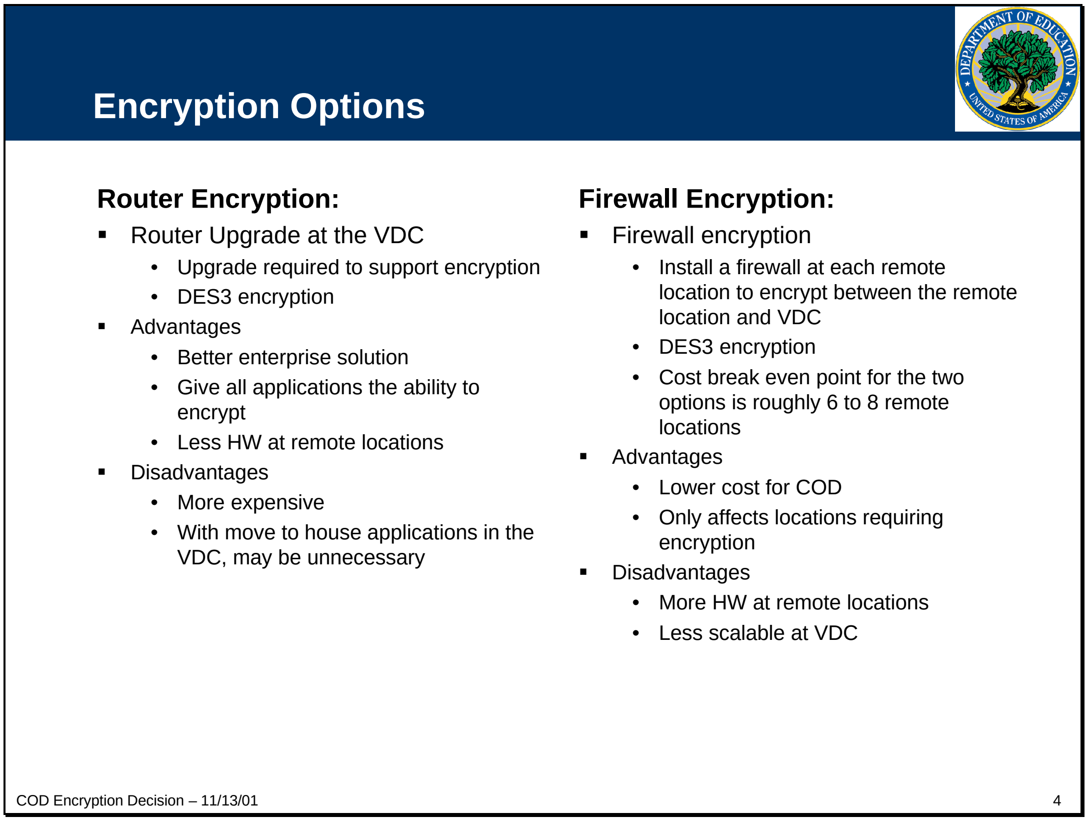
COD Encryption Decision – 11/13/01 2



Government Regulations

- **Privacy Act**
  - Agencies must: "...establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."
  - "(4) In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of--
    - (A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of $1,000; and
    - (B) the costs of the action together with reasonable attorney fees as determined by the court."
- **SFA Extranet Policy**
  - Security policy: Confidential information should be protected when communicated over open networks.
  - If the SFA extranet will allow viewing and/or transfer of confidential information (business units to decide on confidentiality of all but Privacy Act data), then some sort of protection is required.

COD Encryption Decision – 11/13/01 3



Encryption Options

Router Encryption:

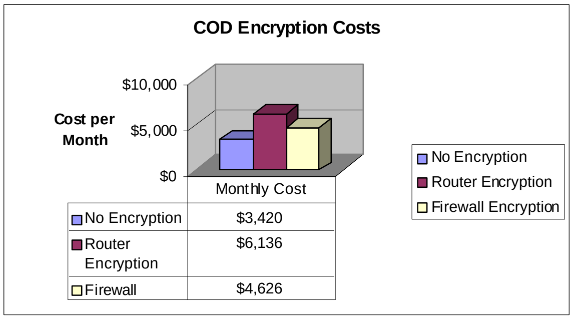
- Router Upgrade at the VDC
  - Upgrade required to support encryption
  - DES3 encryption
- Advantages
  - Better enterprise solution
  - Give all applications the ability to encrypt
  - Less HW at remote locations
- Disadvantages
  - More expensive
  - With move to house applications in the VDC, may be unnecessary

Firewall Encryption:

- Firewall encryption
  - Install a firewall at each remote location to encrypt between the remote location and VDC
  - DES3 encryption
  - Cost break even point for the two options is roughly 6 to 8 remote locations
- Advantages
  - Lower cost for COD
  - Only affects locations requiring encryption
- Disadvantages
  - More HW at remote locations
  - Less scalable at VDC

COD Encryption Decision – 11/13/01 4

Cost Comparison Summary



	Monthly Cost
🟦 No Encryption	$3,420
🟥 Router Encryption	$6,136
🟨 Firewall	$4,626

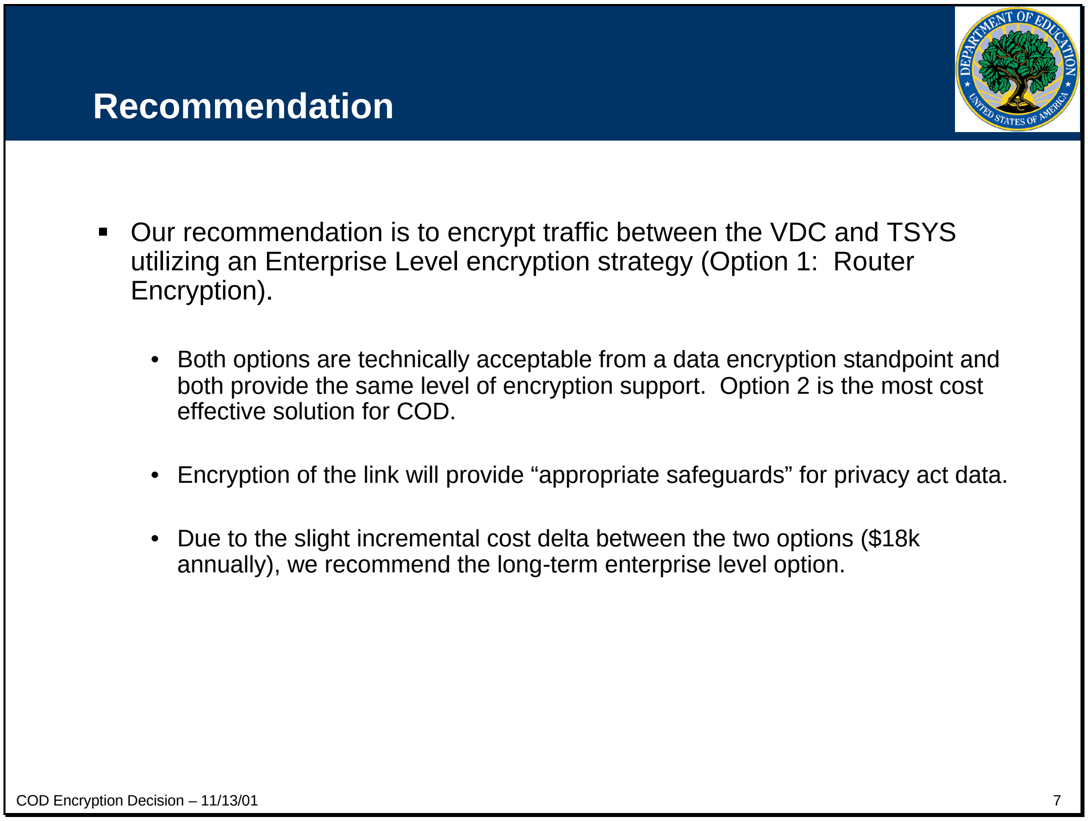
- Base cost = $3420 / mo. VDC charge for no encryptionf
- Firewall based option is $3626 / mo., a $1206 / mo. increase over no encryption
- Router based option is $6136 / mo., a $2716 / mo. increase over no encryption

COD Encryption Decision – 11/13/01 5

Cost Comparison

- Base COD Network Costs
  - Base remote location VDC cost for COD is $3420 / month
  - Only one COD connection would require encryption - VDC to TSYS
    - All the others are web traffic and secured using SSL
- Option 1 Costs:
  - $6136 / mo. per remote location
  - $73,632 annual cost
  - Cost difference from base cost is $2716 / mo., $32,592 per year
- Option 2 Costs:
  - $4626 / mo. per remote location
  - $55,512 annual cost
  - Cost difference from base cost is $1206 per mo., $14,472 per year
    - Cost savings of $18,120/yr. over Option 1

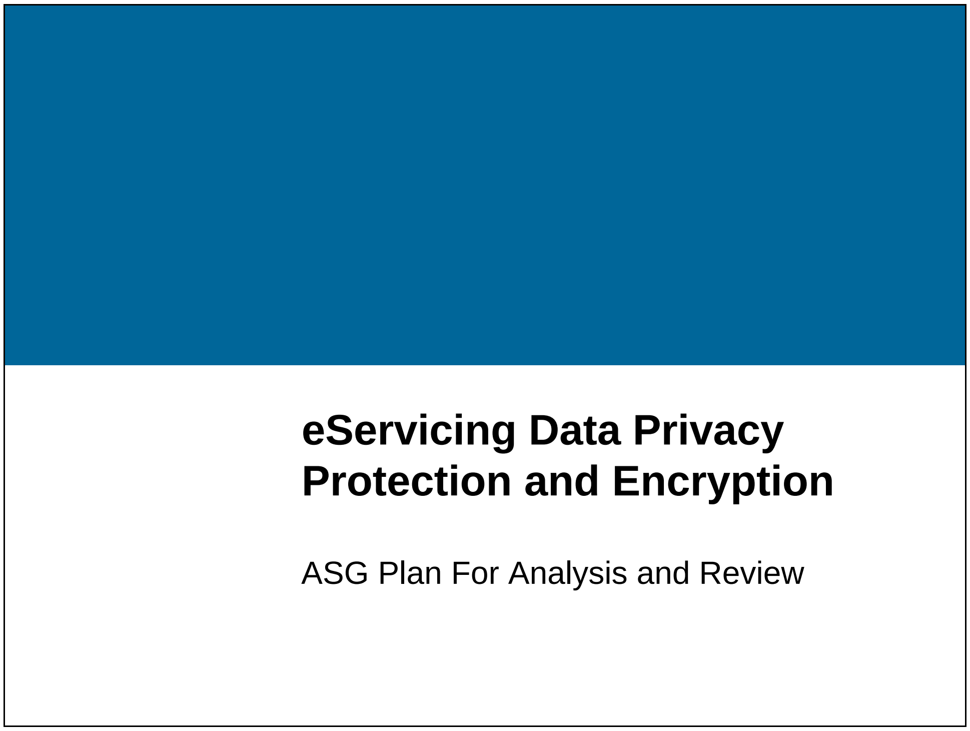
COD Encryption Decision – 11/13/01 6



Recommendation

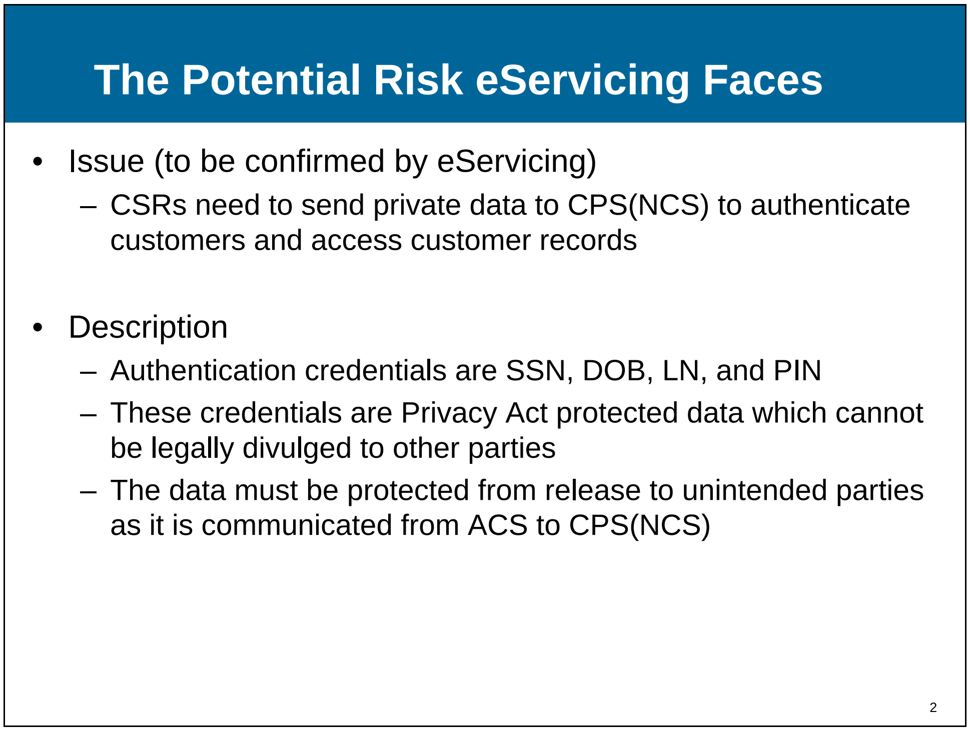
- Our recommendation is to encrypt traffic between the VDC and TSYS utilizing an Enterprise Level encryption strategy (Option 1: Router Encryption).
  - Both options are technically acceptable from a data encryption standpoint and both provide the same level of encryption support. Option 2 is the most cost effective solution for COD.
  - Encryption of the link will provide “appropriate safeguards” for privacy act data.
  - Due to the slight incremental cost delta between the two options ($18k annually), we recommend the long-term enterprise level option.

COD Encryption Decision – 11/13/01 7



eServicing Data Privacy Protection and Encryption

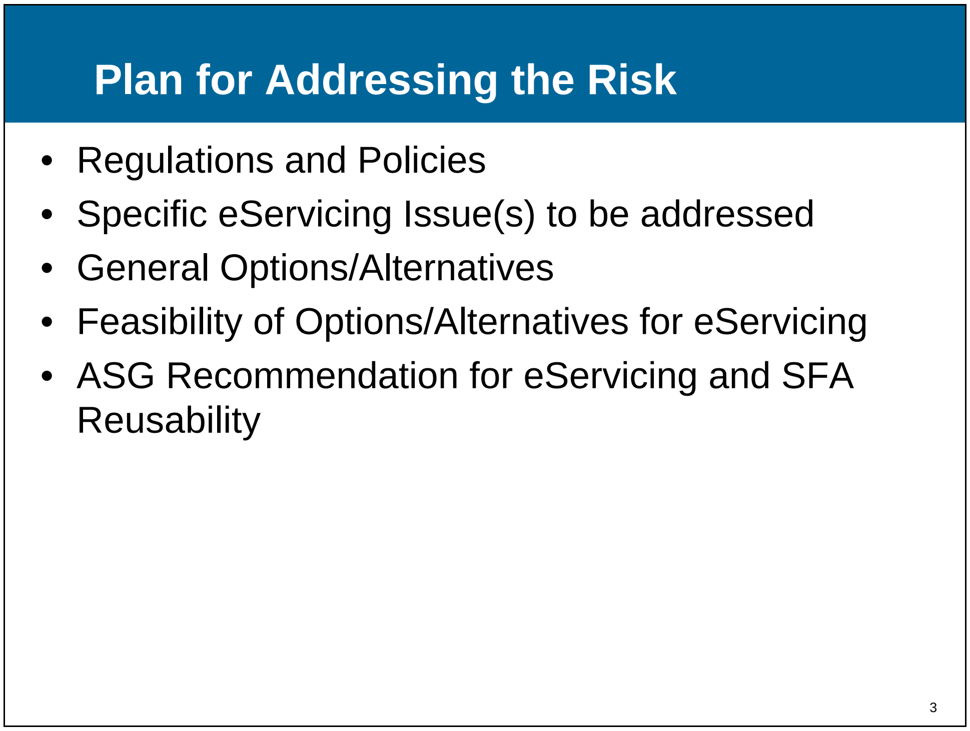
ASG Plan For Analysis and Review



The Potential Risk eServicing Faces

- Issue (to be confirmed by eServicing)
  - CSRs need to send private data to CPS(NCS) to authenticate customers and access customer records
- Description
  - Authentication credentials are SSN, DOB, LN, and PIN
  - These credentials are Privacy Act protected data which cannot be legally divulged to other parties
  - The data must be protected from release to unintended parties as it is communicated from ACS to CPS(NCS)

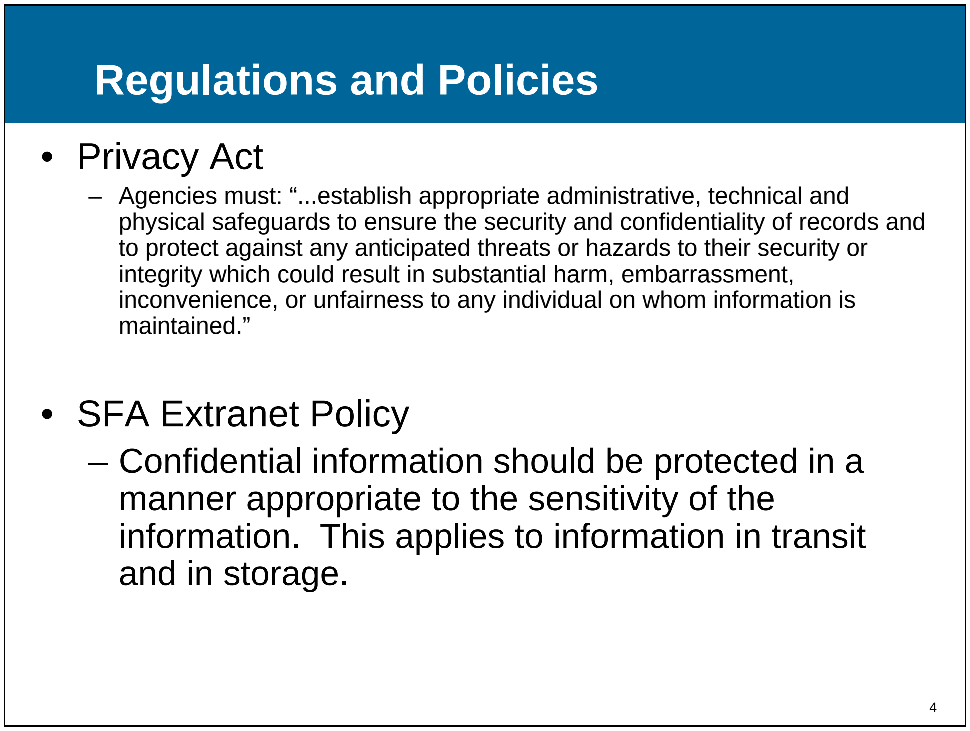
2



Plan for Addressing the Risk

- Regulations and Policies
- Specific eServicing Issue(s) to be addressed
- General Options/Alternatives
- Feasibility of Options/Alternatives for eServicing
- ASG Recommendation for eServicing and SFA Reusability

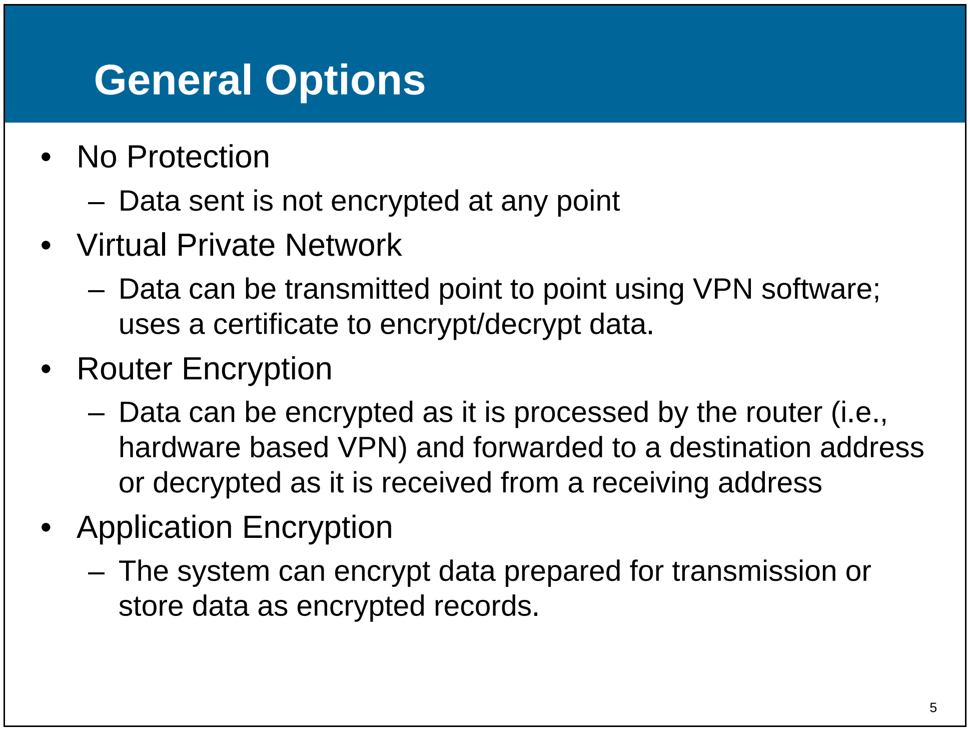
3



Regulations and Policies

- Privacy Act
  - Agencies must: “...establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.”
- SFA Extranet Policy
  - Confidential information should be protected in a manner appropriate to the sensitivity of the information. This applies to information in transit and in storage.

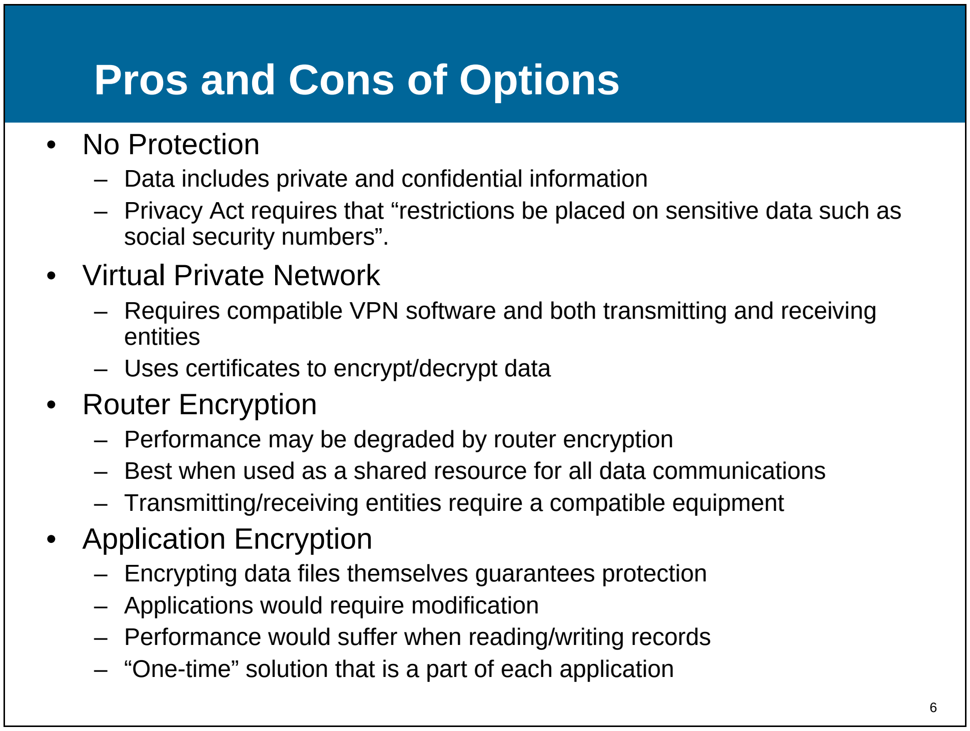
4



General Options

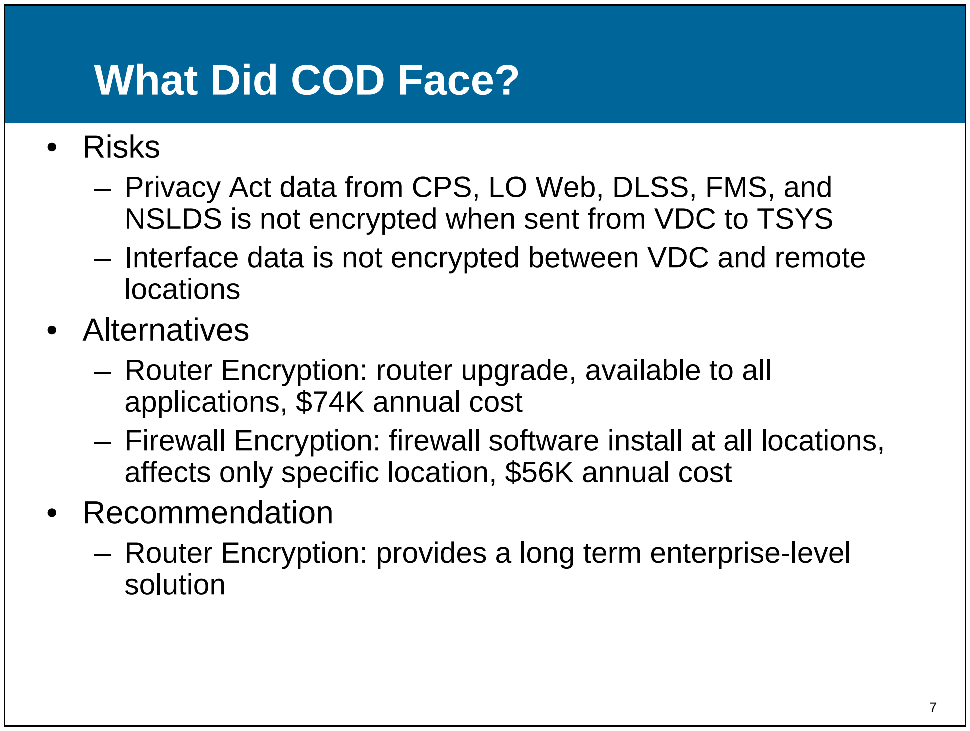
- No Protection
  - Data sent is not encrypted at any point
- Virtual Private Network
  - Data can be transmitted point to point using VPN software; uses a certificate to encrypt/decrypt data.
- Router Encryption
  - Data can be encrypted as it is processed by the router (i.e., hardware based VPN) and forwarded to a destination address or decrypted as it is received from a receiving address
- Application Encryption
  - The system can encrypt data prepared for transmission or store data as encrypted records.

5



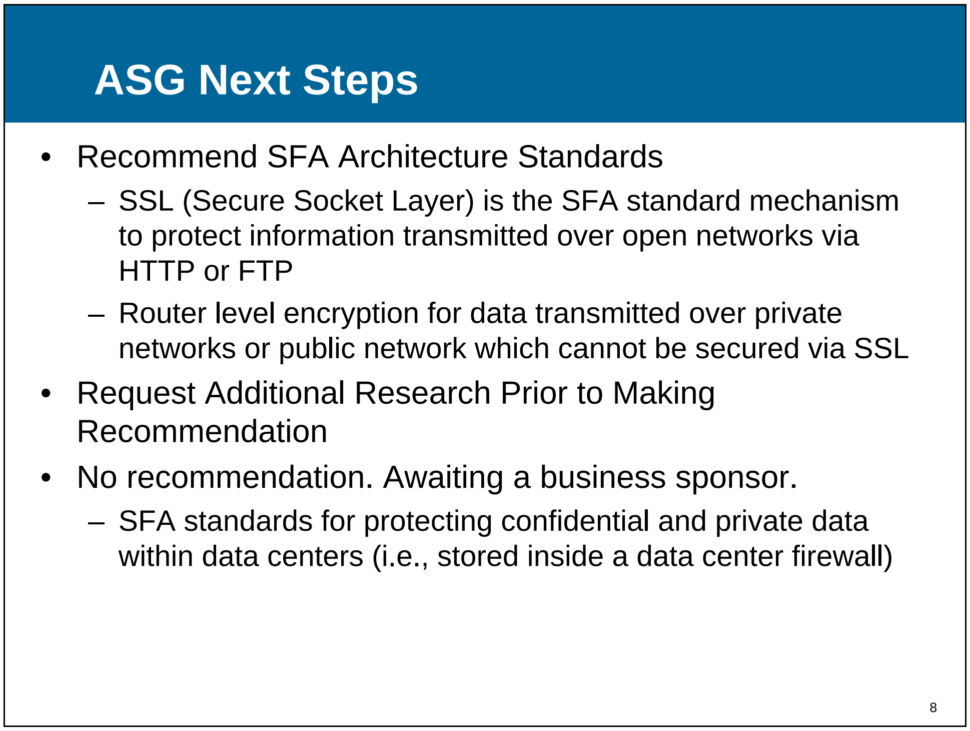
Pros and Cons of Options

- No Protection
  - Data includes private and confidential information
  - Privacy Act requires that “restrictions be placed on sensitive data such as social security numbers”.
- Virtual Private Network
  - Requires compatible VPN software and both transmitting and receiving entities
  - Uses certificates to encrypt/decrypt data
- Router Encryption
  - Performance may be degraded by router encryption
  - Best when used as a shared resource for all data communications
  - Transmitting/receiving entities require a compatible equipment
- Application Encryption
  - Encrypting data files themselves guarantees protection
  - Applications would require modification
  - Performance would suffer when reading/writing records
  - “One-time” solution that is a part of each application



What Did COD Face?

- Risks
  - Privacy Act data from CPS, LO Web, DLSS, FMS, and NSLDS is not encrypted when sent from VDC to TSYS
  - Interface data is not encrypted between VDC and remote locations
- Alternatives
  - Router Encryption: router upgrade, available to all applications, $74K annual cost
  - Firewall Encryption: firewall software install at all locations, affects only specific location, $56K annual cost
- Recommendation
  - Router Encryption: provides a long term enterprise-level solution



ASG Next Steps

- Recommend SFA Architecture Standards
  - SSL (Secure Socket Layer) is the SFA standard mechanism to protect information transmitted over open networks via HTTP or FTP
  - Router level encryption for data transmitted over private networks or public network which cannot be secured via SSL
- Request Additional Research Prior to Making Recommendation
- No recommendation. Awaiting a business sponsor.
  - SFA standards for protecting confidential and private data within data centers (i.e., stored inside a data center firewall)

8

Appendix C: Definitions

Accountability – A high confidence exists that those accessing or changing information are persons and agents properly authorized.

At Rest – Information is stored in some media for future processing or transmission

Availability – Information is available when needed

Confidentiality – Information can only be viewed by persons/agents with appropriate security clearance and "need to know"

Integrity – Information is correct and can be changed only by those authorized to make changes

In Transit – Information that is being moved or copied from one physical/logical location on the network to another

Processing – Information that is being manipulated or viewed by a user or application program on a host platform